#15

Patent 1083

IN THE U.S. PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicant: KOICHI KAMIJO et al.	:	Group Art Unit: 2134
Serial No.: 09/459,287	:	Examiner: Michael J. Simitoski
Filed: December 17, 1999	:	August 23, 2004
Confirmation No.: 9962	:	William A. Kinnaman, Jr.
Title: SYSTEM FOR AUTHENTICATING	:	International Business Machines Corporation
DIGITAL DATA	:	2455 South Road, Mail Station P386
	:	Poughkeepsie, NY 12601

RECEIVED
2004 AUG 25 PM 3:39
BOARD OF PATENT APPEALS AND INTERFERENCES

APPLICANTS' APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RECEIVED
SEP 01 2004
Technology Center 2100

Dear Sir:

09/13/2004 VJUAN1 00000001 09459287
01 FC:1402 330.00 DA

Applicants hereby submit their appeal brief in the above-identified application.

CERTIFICATE OF MAILING UNDER 37 CFR 1.8(a)

I hereby certify that this correspondence is being deposited in triplicate with the United States Postal Service as first-class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on August 23, 2004.

Sandra L. Kilmer

Sandra L. Kilmer

August 23, 2004

Date:

REAL PARTY IN INTEREST

The real party in interest is International Business Machines Corporation, the assignee of record.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

Claims 1-5, 8 and 10-22 stand rejected and are on appeal. Claim 30 has been allowed. Claims 6-7, 9 and 23-29 have been cancelled.

STATUS OF AMENDMENTS

An amendment after final rejection filed April 19, 2004, cancelling claims 23-29 and presenting claim 30 in independent form, has been entered. There are no other amendments after final rejection.

SUMMARY OF INVENTION

The invention relates to the authentication of digital data in a system for writing digital data entered from an input device 100 such as a digital camera (Fig. 1) to a memory device 200 and transferring the digital data written in the memory device 200 to a receiving device 300 such as a personal computer (PC). In accordance with the invention, a first device authentication is performed between the input device 100 and the memory device 200 when writing digital data from the input device 100 to the memory device 200 (page 5, steps 1.1-1.5), while a second device authentication is performed between the memory device 200 and the receiving device 300 when transferring the digital data from the memory device to the receiving device 300 (pages 7-8, steps 3.1-3.7).

In the first device authentication, the input device 100 requests from the memory device 200 a random number R1 (step 1.1), which the memory device 200 returns to the input device 100 (step 1.2). After starting data transfer (step 1.3), the input device 100 encrypts the random number R1 using an encryption function

$$R\_Ed = Hdc(Kdc, R1),$$

where R_Ed is the encrypted value and Kdc is a secret key shared with the memory device 200, and returns the encrypted value R_Ed to the memory device 200 (step 1.4). The memory device 200 compares the received R_Ed value with an R_Ed value generated by it using its own copies of R1 and Kdc (step 1.5). If the two values match, the memory device 200 treats the transferred data as authenticated data by attaching an authentication flag and generating a digital signature on the data. Otherwise, the memory device 200 treats the data as ordinary data.

In the second device authentication, the receiving device 300 sends the memory device 200 a random number R2 (steps 3.1-3.2). The receiving device 300 then starts reading data from the memory device (step 3.3). The memory device 200 then encrypts the random number R2 using an encryption function

$$R\_Ep = Hpc(Kpc, R2),$$

where R_Ep is the encrypted value and Kpc is a secret key shared with the receiving device 300, and returns the encrypted value R_Ep to the receiving device 300 (step 3.5). The receiving device 300 compares the received R_Ep value with an R_Ep value generated by it using its own copies of R2 and Kpc (step 3.6). If the two values match, the data is considered authenticated. The receiving device 300 sends a seed the memory device for each subsequent read operation, and an authentication procedure similar to the one described above is performed (step 3.7). Only if all such authentication operations are performed successfully is the data considered authenticated.

ISSUES

I. Whether claims 1-3, 5, 8, and 10-22 were properly rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent 6,510,520 to Steinberg in view of U.S. Patent 5,949,877 to Traw et al. ("Traw"), either alone or in further view of Schneier, Applied Cryptography, Second Edition ("Schneier").

II. Whether claim 4 was properly rejected under 35 U.S.C. § 103 as being unpatentable over Steinberg in view of Traw and U.S. Patent 5,465,300 to Altschuler et al. ("Altschuler").

GROUPING OF CLAIMS

Separately argued below are: (1) claims 1-3, 5, 8, and 10-22; and (2) claim 4.

ARGUMENT

Claims 1-3, 5, 8, and 10-22

This group of claims on appeal is based upon three independent claims: claims 1, 15 and 21. Claim 1 is representative of this group and reads as follows:

> 1. A method for authenticating digital data in a system for writing digital data entered from an input device to a memory device and transferring the digital data written in the memory device to a receiving device, said method comprising the steps of:
>
> performing a first device authentication between the input device and the memory device when writing digital data from the input device to the memory device; and
>
> performing a second device authentication between the memory device and the receiving device when transferring the digital data from the memory device to the receiving device.

Claim 15 is similar to claim 1, but is directed to apparatus. Claim 21 is similar to claim 15, but is directed to a memory device and recites that the memory device comprises means for performing the first and second device authentications.

Claims 1-3, 5, 8, 10-12, 14-19 and 21 stand rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent 6,510,520 to Steinberg in view of U.S. Patent 5,949,877 to Traw et al. ("Traw") (paper no. 9, page 2, ¶ 3). Claims 13, 20 and 22 stand rejected under 35 U.S.C. § 103 as being unpatentable over Steinberg in view of Traw and Schneier, Applied Cryptography, Second Edition ("Schneier") (paper no. 9, page 4, ¶ 5). For the reasons stated below, these rejections are untenable and should be reversed.

Each of the claims on appeal is directed to a method, apparatus or memory device, as the case may be, in which a first device authentication is performed between an input device and an memory device when writing digital data from the input device to the memory device, while a second device authentication is performed between the memory device and the receiving device when transferring the digital data from the memory device to the receiving device.

Steinberg discloses a digital camera system in which a secure storage device 10 (Fig. 1) intermediating between a digital camera 14 and a user's personal computer (PC) 16 is used to either encrypt a digital image or generate a signature on the image. The ultimate user, not the secure storage device, either decrypts the image or authenticates the digital signature, depending on the type of processing performed by the secure storage device.

Traw discloses a method for protecting digital content from "copying and/or other misuse" as it is transferred between devices over insecure links; the method includes the step of authenticating that both a content source and a content sink are compliant devices (col. 1, lines 42-48). In the mutual authentication procedure shown in Figs. 1(a)-1(c), each device sends the other device a signed message, which the receiving device authenticates by verifying the signature of the sending device, together with other actions.

Schneier, cited only against claims 13, 20 and 22 and whose application to those claims is not challenged in this appeal, teaches the use of a message authentication code (MAC) by a single user to determine whether data stored by the user has been altered (pages 455-456, § 18.14).

The Examiner concedes that Steinberg does not disclose authenticating between his input device and memory device and between his memory device and receiving device, but argues that Traw teaches "that copying and/or other misuse of data being transferred can be prevented by performing a first device authentication between a content source and a content sink" (paper no.9, page 3). The Examiner concludes from this that it would have been obvious to perform a first device authentication between Steinberg's input device and memory device and a second device authentication between his memory device and the receiving device "to prevent copying and/or misuse of the data during transfer" (paper no. 9, page 3). Applicants respectfully disagree.

Applicants are not concerned with "copying and/or other misuse" of data, as were Traw and his co-inventor. Indeed, in the disclosed embodiments applicants' digital data is transmitted and stored in the clear (i.e., in unencrypted form), so that anyone with physical access to the memory device can access the data. Rather, applicants are concerned with authenticating such data and protecting it against alteration by someone seeking, for example, to perpetrate an insurance fraud (specification, page 1). It is not at all apparent why one concerned with guarding against data alteration would look to a copy protection mechanism for guidance. Accordingly, one cannot properly combine Steinberg with Traw to obtain applicants' invention.

Claim 4

Claim 4, dependent on claim 1, reproduced above, recites that the digital data is transferred as authenticated data if the first and second device authentications are successful and is transferred as ordinary (i.e., unauthenticated) data (page 3, lines 14-15) if the first and second device authentications are not successful. This corresponds to the described mode of operation in which the data transfer is either ordinary or authenticated, with an authentication flag being set to mark the difference (page 5, lines 19-22), depending on the results of device authentication (page 5, steps 1.1-1.2 and 1.5).

Claim 4 stands rejected under 35 U.S.C. § 103 as being unpatentable over Steinberg in view of Traw and U.S. Patent 5,465,300 to Altschuler et al. ("Altschuler") (paper no. 9, page 4, ¶ 4).

Altschuler discloses a so-called secure communication setup method, whereby a "secure" (i.e., encrypted) call setup procedure 54 (Fig. 6) is automatically invoked after a handshaking sequence that may include an initial plaintext communication session. The disclosed method is said to constitute an improvement over existing methods in which the transition from a plaintext session to a secure session depends on the voluntary act of a human operator (col. 1, lines 39-53).

The Examiner argues that it would have been obvious in view of Altschuler to further modify Steinberg "to include a means for automatically determining whether or not to use secure communication methods"; one would have been motivated to do so, the Examiner adds, "to eliminate the need for human decision, as taught by Altschuler" (paper no. 9, page 4, ¶ 4). This is simply incorrect, for at least two reasons.

First, while both Altschuler and applicants use the term "secure",[1] they use it very differently in reference to their respective systems. In Altschuler, the concern is data privacy, and the relevant dichotomy is between plaintext and encrypted modes of communication. Communications are "secure" in Altschuler's system if they are encrypted. In applicants' claimed system, on the other hand, the concern is data integrity (page 2, lines 1-3), and the relevant dichotomy is between unauthenticated (i.e., "ordinary") and authenticated data transfer.

An authenticated data transfer differs from an unauthenticated data transfer not because it is encrypted—applicants' data remains unencrypted in either transfer mode—but because it is authenticated as having originated from a definite source and as not having been altered in the course of its transmission and storage. The mere fact that a communication has been encrypted says nothing about whether it is authentic. Indeed, if a public key cryptosystem is used, anyone

[1] Applicants use this term in the specification, but not at all in the claims, where instead they use the more precise term "authenticated".

with access to the encryption key of the recipient—and this is basically everyone in public key system—will be able to send an encrypted message to the receiver.

Accordingly, since Altschuler is concerned with data privacy rather than data integrity, no one seeking to improve a data authentication system would be motivated to consult this reference for a relevant teaching.

Second, whatever meaning one attaches to the term "secure", Altschuler always transitions from an insecure mode of communication to a secure mode of communication, so that at the end of the secure call setup procedure, the parties are communicating either securely (if the setup procedure succeeded) or not at all (if the setup procedure failed). That is to say, Altschuler does not use a secure mode of communication if his setup procedure succeeds while using an insecure mode of communication if his setup procedure fails, as claimed by applicants.[2]

Therefore, even if Steinberg and Traw were deemed to teach the subject matter of claim 1, and that subject matter were modified as allegedly suggested by Altschuler, the resulting system would not transfer digital data as authenticated data if the device authentications are successful and as ordinary data if the device authentications are not successful, as recited in claim 4. Rather, if the authentication procedure failed, no further data transfer, "ordinary" or otherwise, would take place.

Thus, not only would it not be obvious to combine the teachings of Altschuler with those of Steinberg and Traw, but even if they were combined, the resulting combination would not be what is claimed in claim 4. Accordingly, claim 4 distinguishes patentably over the art cited by virtue of its additional recitations, as well as for the reasons urged above with respect to claim 1.

[2] Claim 4 does not use this language but implies this mode of operation, which is all that is relevant to the point under discussion.

Conclusion

For the foregoing reasons, claims 1-5, 8 and 10-22 distinguish patentably over the references cited by the Examiner. The Examiner's rejection of these claims is therefore untenable and should be reversed.

Respectfully submitted,
KOICHI KAMIJO et al.

By 

William A. Kinnaman, Jr.
Registration No. 27,650
Phone: (845) 433-1175
Fax: (845) 432-9601

WAK/wak

APPENDIX

Claims on Appeal[3]

1. A method for authenticating digital data in a system for writing digital data entered from an input device to a memory device and transferring the digital data written in the memory device to a receiving device, said method comprising the steps of:

performing a first device authentication between the input device and the memory device when writing digital data from the input device to the memory device; and

performing a second device authentication between the memory device and the receiving device when transferring the digital data from the memory device to the receiving device.

2. The method of claim 1 comprising the step of:

mixing data for performing device authentication into the digital data written from said input device to said memory device and the digital data transferred from said memory device to said receiving device.

3. The method of claim 1 wherein said second device authentication is performed by a central processing unit built into said memory device.

4. The method of claim 1 wherein said digital data is transferred as authenticated data if said first and second device authentications are successful and is transferred as ordinary data if said first and second device authentications are not successful.

5. The method of claim 1 wherein said first device authentication is performed using a first encryption function and key and said second device authentication is performed using a second encryption function and key.

6-7. (Cancelled)

[3] Listing also indicates cancelled claims and includes allowed claim 30.

8. The method of claim 1 wherein said device authentication between said input device and said memory device is performed by using a public key system.

9. (Cancelled)

10. The method of claim 1 wherein each of said device authentications involves having a first device ascertain that a second device possesses a secret value corresponding to a value held by the first device.

11. The method of claim 10 wherein the first device is a recipient of digital data from the second device.

12. The method of claim 1 wherein each of said device authentications involves the exchange of an authentication value generated independently of said digital data.

13. The method of claim 1, comprising the further steps, performed by the memory device, of:

generating an electronic signature on the digital data when writing the digital data from the input device to the memory device; and

authenticating the electronic signature on the digital data when transferring the digital data from the memory device to the receiving device.

14. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform the method steps of claim 1.

15. Apparatus for authenticating digital data in a system for writing digital data entered from an input device to a memory device and transferring the digital data written in the memory device to a receiving device, said apparatus comprising:

means for performing a first device authentication between the input device and the memory device when writing digital data from the input device to the memory device; and

means for performing a second device authentication between the memory device and the receiving device when transferring the digital data from the memory device to the receiving device.

16. The apparatus of claim 15 wherein said means for performing said second device authentication comprises a central processing unit built into said memory device.

17. The apparatus of claim 15 wherein said first device authentication is performed using a first encryption function and key and said second device authentication is performed using a second encryption function and key.

18. The apparatus of claim 17 wherein said encryption functions and said first key are stored in a read-only memory of said memory device.

19. The apparatus of claim 17 wherein said second key is encrypted and stored in NAND record space.

20. The apparatus of claim 15, further comprising:

means associated with the memory device for generating an electronic signature on digital data when writing the digital data from the input device to the memory device; and

means associated with the memory device for authenticating the electronic signature on the digital data when transferring the digital data from the memory device to the receiving device.

21. A memory device for authenticating digital data in a system for writing digital data entered from an input device to the memory device and transferring the digital data written in the memory device to a receiving device, said memory device comprising:

means for performing a first device authentication with the input device when writing digital data from the input device; and

means for performing a second device authentication with the receiving device when transferring the digital data to the receiving device.

22. The memory device of claim 21, further comprising:

means for generating an electronic signature on the digital data when writing the digital data from the input device to the memory device; and

means for authenticating the electronic signature on the digital data when transferring the digital data from the memory device to the receiving device.

23-29. (Cancelled)

30. (Allowed) A memory device for authenticating digital data in a system for writing digital data entered from an input device to the memory device and transferring the digital data written in the memory device to a receiving device, said memory device comprising:

means for generating an electronic signature on digital data when writing the digital data from the input device;

means for storing the digital data and the electronic signature; and

means for authenticating the electronic signature on the digital data when transferring the digital data to the receiving device, wherein said memory device is a flash memory and stores said electronic signature on said digital data in a redundant area not to be calculated by an ECC of each page in a memory area.